事例で学ぶセキュリティインシデント（第4回）

メール攻撃を防ぐための原則は「不審な添付ファイルは開かない」

2023.09.19

「朝早くからすみません。支店に届いたメールの内容がいつもと違うようです。見てもらえませんか」

D社のIT担当者に支店従業員から電話があったのは、始業直後。「標的型メール攻撃かもしれない」。IT担当者は、日頃から不審なメールが届いたらすぐに連絡するように社内通達していた。そして、パソコンをネットワークから切り離し、本社まで持参するように伝えた。

取引先を詐称した偽の案内メールを受信

D社は関西に複数店舗を展開する不動産会社だ。ファミリー向けの賃貸マンションや貸店舗などを手掛け、社員は約40名の企業だが、地域に密着した事業展開で成長してきた。管理部門の社員がIT担当を兼務しており、物件の賃貸借にかかわる顧客の個人情報を扱うことから情報セキュリティ対策に力を入れてきた経緯がある。

D社のシステムと情報セキュリティをサポートするIT事業者の助言もあり、社内ネットワークとインターネットとの境界にファイアウォールやウイルス対策ソフトを導入。この他、「不審なメールは開かない」といった通達の徹底など従業員の安全意識向上にも取り組んできた。

IT担当者は、IT事業者の協力を得ながら問題のパソコンのメールを調べた。メールの送り主は取引先の住宅会社と同じ名称だ。メールのタイトルは「新規物件のご案内」。文面は通常のあいさつの他、新規物件を紹介するWebサイトのURLが記載されていた。いつも新規物件の案内はPDFファイルが添付されており、URL記載はなかった。メールを受信した支店担当者は取引先にメールを送ったかどうか確認する方法もあったが、送信元社名が正しかったため、「変なことを尋ねたら、失礼になる」と考え、本社のIT担当者に電話したという。

IT担当者がURLを調べたところ、取引先のものではなく、海外にあるWebサイトであった。万一、そのURLをクリックすればウイルスに感染する恐れもある標的型メール攻撃の可能性が高いと判断した。

メールの情報が盗まれ感染拡大の恐れも… 続きを読む